03-0340

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION FOR PATENT

ON

3-PRONG SECURITY/RELIABILITY/REAL-TIME DISTRIBUTED ARCHITECTURE OF INFORMATION HANDLING SYSTEM

BY

CHRISTOPHER HAMLIN
310 JENSEN SPRINGS RD
LOS GATOS, CA 95033
CITIZEN OF USA

CERTIFICATE OF MAILING BY "EXPRESS MAIL"

"Express Mail" Mailing Label Number EV 338 283 888 US

Date of Deposit: August 4, 2003

I hereby certify that this correspondence is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 C.F.R. § 1.10 on the date indicated above and is addressed to MS Patent Application Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

BY: ReNea D. Berggren

ReNea D. Berggren

3-PRONG SECURITY/RELIABILITY/REAL-TIME DISTRIBUTED ARCHITECTURE OF INFORMATION HANDLING SYSTEM

FIELD OF THE INVENTION

[0001] This invention relates generally to an information handling system, and particularly to a 3-prong security/reliability/real-time distributed architecture for an information handling system.

BACKGROUND OF THE INVENTION

[0002] There are three well known fundamental problems in an information handling system: security, reliability, and real-time behavior. Security refers to a system's ability to prevent unauthorized agents from performing actions while permitting authorized agents to perform actions. Security is related to data protection and privacy, and especially related to digital rights management (DRM). Reliability refers to a system's robustness in handling information. Real-time behavior refers to a system's ability to update information as the information is received, enabling the system to direct or control processes. It is understood that an information handling system here is defined as a group of related components that interact to process information. An information handling system may be hardware only, software only, or a combination of hardware and software.

[0003] Traditional solutions to the foregoing-indicated three problems have emphasized on solving each problem separately. However, this approach is sub-optimal from both an architectural and an economic point of view, as it fails to exploit the synergies of the interdependence an architecture may provide.

[0004] A legacy architecture of an information handling system, that is, a traditional microprocessor and operating system structure (e.g., UNIX or Microsoft Windows running on an Intel processor), is inherently insecure and is also not scalable. Therefore,

a legacy architecture applies very poorly to a distributed environment scaled both in the number of supported devices and in behavior or performance.

[0005] Thus, it would be desirable to provide an architecture for an information handling system which simultaneously addresses security, reliability, and real-time behavior problems inherent in the known art, while also solving legacy architecture scalability and security problems.

SUMMARY OF THE INVENTION

[0006] Accordingly, the present invention is directed to a distributed architecture of an information handling system which addresses security, reliability, and real-time behavior problems. In one aspect of the present invention, a 3-prong security/reliability/real-time distributed architecture in accordance with the present invention may have one or more of the following features: (1) system solutions; (2) characterizability; (3) architectural independence of implementation means; (4) interdependence of functions; (5) security characterization; (6) quasi-stability; (7) buried nucleus; (8) adaptation; (9) reliability; (10) secure protocol; (11) ability to rebuild after intrusion; and (12) isochronous real-time foundation.

[0007] In an additional aspect of the present invention, a distributed architecture of an information handling system includes a buried nucleus inaccessible for inspection without heroic means while the buried nucleus is in operation, and a trusted authority for generating a secure protocol. The secure protocol may control the operation of the buried nucleus.

[0008] In another aspect of the present invention, a distributed architecture of an information handling system includes a hardware/software system, and a trusted authority for generating a secure protocol. The secure protocol may control the operation of the hardware/software system. Preferably, the hardware/software system includes a

microchip which includes a buried nucleus and an outer region having I/O pins. The hardware/software system may further include external software connected to I/O pins for controlling I/O pins. The buried nucleus may also be equipped to accept and decipher an encrypted key delivered through a secure protocol. An operating buried nucleus may not be accessible for inspection without heroic means.

[0009] In a further aspect of the present invention, a method for protecting encrypted information on a network from, for example, a grid dribble attack, includes the following steps: (1) setting a buried nucleus in a quasi-stable mode of operation; (2) stopping clocking when the buried nucleus deviates from the quasi-stable mode; (3) rebuilding a secure environment within the buried nucleus after an intrusion is detected; and (4) stopping clocking when replication of re-buildup by an attacker is detected.

[0010] It should be understood the foregoing general description and following detailed description are exemplary and explanatory only and are not restrictive of the invention as claimed. The accompanying drawings, which are incorporated in and constitute a part of the specification, illustrate an embodiment of the invention and together with the general description, serve to explain the principles of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] The numerous advantages of the present invention may be better understood by those skilled in the art by reference to the accompanying figures in which:

FIG. 1 is a schematic diagram illustrating a three-dimension cost/threat/risk space;

FIG. 2 is a simplified block diagram of an exemplary hardware/software instantiation of a 3-prong security/reliability/real-time distributed architecture in accordance with the present invention;

FIG. 3 shows a derivative approach (grid dribble attack) to violating copyright on a digital medium; and

FIG. 4 is a flowchart illustrating an exemplary process for protecting against a grid dribble attack in accordance with an exemplary embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0012] Reference will now be made in detail to the presently preferred embodiments of the invention, examples of which are illustrated in the accompanying drawings.

[0013] According to one aspect of the present invention, a secure distributed structure may only be founded on a secure base. Likewise, a secure distributed structure may not be retrofitted to an insecure base such as a legacy architecture (whether in hardware or software). Furthermore, large networks of secure digital clients require such a foundation.

I. ARCHITECTURE FEATURES

[0014] The 3-prong security/reliability/real-time distributed architecture in accordance with the present invention may have one or more of the following features: (1) system solutions; (2) characterizability; (3) architectural independence of implementation means; (4) interdependence of functions; (5) security characterization; (6) quasi-stability; (7) buried nucleus; (8) adaptation; (9) reliability; (10) secure protocol; (11) ability to rebuild after intrusion; and (12) isochronous real-time foundation.

(1) System Solutions

[0015] Although the three functions (security, reliability, and real-time behavior) are susceptible to individual point solutions, these point solutions are distinctly sub-optimal from both an architectural and an economic point of view and fail to exploit the synergies of interdependence an architecture may provide.

[0016] According to the present invention, the triad of functional objectives (security, reliability, and real-time behavior) may be synergistic and may therefore best be achieved simultaneously in a 3-prong security/reliability/real-time distributed architecture, which unifies the means employed for each objective as the basis for cost-effective scalability. That is, rather than treating security, reliability, and real-time behavior as independent point problems or independent point solutions, the three areas may be treated as interrelated problems that share certain common underlying architectural features.

(2) Characterizability

[0017] Any instantiation of a 3-prong security/reliability/real-time distributed architecture of the present invention may be characterizable in each function domain (security, reliability, or real-time behavior).

[0018] The characterization of the present invention is extremely important and very fundamental because many point solutions in this phase which are available today are extremely difficult to characterize, forcing construction of over built, inefficient, problematic, and over provisioned solutions. One must apply more resources to solving the problem than required from a systems point of view.

(3) Architectural Independence of Implementation Means

[0019] According to a preferred embodiment of the present invention, invariant architecture is independent from characterizable implementations. A fundamental characteristic of the 3-prong security/reliability/real-time distributed architecture of the present invention is that the architecture may be viewed independently of a particular instantiation or implementation. The architecture is invariant. That is, the particular functional characteristics of the architecture in terms of how the architecture actually provides security, how the architecture actually provides real-time behavior, and how the

architecture actually provides reliability, are preferably fixed. However, the extent to which the architecture provides those characteristics in a particular instantiation or implementation may actually be characterized quantitatively. That is, while the architecture remains fixed, variants of the architecture may have very modest resource consumptions or may be very powerful. In this way, the level of performance for the particular characterization may be scaled according to how the present invention is implemented.

[0020] The architecture of the present invention may apply to a distributed environment which is scalable both in the number of supported devices, e.g., from a couple of devices to literally billions of devices, and in behavior or performance. The distributed environment may be a very tiny device, like an embedded behavior or performance. The distributed environment may be a smart card or may be a supercomputer mainframe. The architecture according to the present invention may address that entire scaling range, and may be suitable for a very small numbers of devices or suitable for accommodating very large aggregates of devices with respect to the three fundamental problems of security, reliability and real-time behavior.

[0021] According to the present invention, with fixed architecture, the architecture may be implemented in many ways. The architecture may be implemented entirely in hardware for some purposes, the architecture may be implemented entirely in software for other purposes, or the architecture may be implemented in a combination of hardware and software for yet other markets and allocation sets.

[0022] According to the present invention, the architecture itself may not require a hardware-only, a software-only, or a hardware/software implementation. The characterization of the delivery of security, reliability and real-time behavior in each of those settings may be different and may be characterized differently as a result of the choices made in implementation.

(4) Interdependence of Functions

[0023] The functions of security, reliability, and real-time behavior are interdependent within the architectural structure of the present invention.

(5) Security Characterization

[0024] According to the present invention, security may be characterized based on a formal cost/threat/risk model, where the cost is a cost of implementing a defense against an attack, the risk is a value of an asset that is under attack, and the threat is a level of investment that an attacker is willing to make. According to the present invention, there is really no such thing as an unbreakable system, but instead, the concept of characterization is used to indicate that in a three-dimension space as shown in FIG. 1, one may characterize efficacy of a solution in terms of cost, threat and risk.

[0025] As shown in FIG. 1, a particular instantiation of the 3-prong security/reliability/real-time distributed architecture of the present invention may occupy a position P within a cost/threat/risk space. Thus, for the particular instantiation corresponding to the position P, one is placing an asset with a z amount of value at risk, and one is willing to invest a x amount of cost in ensuring that the asset is protected on the assumption that an attacker is not willing to invest more than a y amount of effort or dollars. All of these things (cost, threat, and risk) may, of course, be expressed in a dollar value.

[0026] It is noted that different instantiations of the 3-prong security/reliability/real-time distributed architecture of the present invention may occupy different positions of the cost/threat/risk space shown in FIG. 1. For example, if an instantiation is an ATM machine, the risk is great because the value of the asset under attack is great, so one would be willing to spend a lot on the protection, and one also has to assume an attacker

would be willing to spend significantly on the attack. However, if all one is trying to protect is an e-mail for one particular day that has an inconsequential content, then cost and risk would be low, and one may not really care if the data are infiltrated by a hacker. The security characterization will be more fully described with the DRM.

(6) Quasi-stability

[0027] The 3-prong security/reliability/real-time distributed architecture of the present invention may have quasi-stability. Cumulative attacks may be thwarted through immediate suspension of operation upon intrusion detection. The quasi-stability will be described in more detail with the DRM.

(7) Buried Nucleus

[0028] Some instantiations of the 3-prong security/reliability/real-time distributed architecture of the present invention may require "buried" hardware resources to achieve the instantiations' security characterization. The buried nucleus concept will be described in more detail with the DRM.

(8) Adaptation

[0029] The 3-prong security/reliability/real-time distributed architecture of the present invention may support adaptive responses to changing conditions either autonomously or under supervision of a remote trusted authority. The adaptation may include self-healing and self-sealing behaviors.

(9) Reliability

[0030] The adaptive responses of the 3-prong security/reliability/real-time distributed architecture of the present invention to failure modes preferably permits continued aggregate functioning of client populations containing failed members, especially in large populations with failed members.

(10) Secure Protocol

[0031] The 3-prong security/reliability/real-time distributed architecture of the present invention may require use of a demonstrably secure adaptive protocol operating peer-to-peer and/or via a trusted authority to manage the system environment and assure system integrity.

(11) Ability to Rebuild after Intrusion

[0032] The 3-prong security/reliability/real-time distributed architecture of the present invention may support re-establishment of a demonstrably secure environment in the face of detected intrusions.

(12) Isochronous Real-Time Foundation

[0033] According to a preferred embodiment of the present invention, real-time functions are predicated on multiple independently synthesizable isochronous paths in the 3-prong security/reliability/real-time distributed architecture.

[0034] It is understood that the foregoing-described features are exemplary only and are not intended to limit the scope of the present invention. Those of ordinary skill in the art will understand that other features may also be included in the architecture of the present invention without departing from the scope and spirit of the present invention.

II. ARCHITECTURE FOR DIGITAL RIGHTS MANAGEMENT (DRM)

[0035] As described above, the 3-prong security/reliability/real-time distributed architecture of the present invention may be implemented entirely in hardware, entirely in software, or in a combination of hardware and software. An exemplary hardware/software instantiation of the architecture of the present invention is described as follows in the context of digital rights management.

(1) Architecture

[0036] DRM poses one of the greatest challenges for content communities in the digital age. Traditional rights management of physical materials benefited from the materials' physicality (as this provided some barrier to unauthorized exploitation of content). However, because of the ease with which digital files may be copied and transmitted, serious breaches of copyright law are not uncommon in a connected society. Thus, one aspect of the DRM focuses on security and encryption as a means of preventing unauthorized copying. That is, DRM tries to lock the content (e.g. a movie in a DVD medium) and limit its distribution to only those paying through an authorization procedure. The level of security provided may be adjusted commensurate to content value.

[0037] Referring now to FIG. 2, a simplified block diagram of an exemplary hardware/software instantiation of a 3-prong security/reliability/real-time distributed architecture 200 in accordance with the present invention is shown. The architecture 200 may increase the security for DRM purposes. The architecture 200 includes a hardware/software system 202, and a trusted authority 206 that generates a secure protocol 204. The secure protocol 204 may control the operation of the hardware/software system 202.

[0038] The hardware/software system 202 preferably includes a microchip 208 and software 210. The microchip 208 preferably includes a buried nucleus (BN) 212 and an outer region 214. The outer region 214 is the area of the microchip 208 other than the BN 212 and includes all the I/O (input/output) pins and pads of the microchip 208. The I/O pins of the microchip 208 are connected to the external software 210 which manipulates or controls these I/O pins.

[0039] The BN 212 may include resource sets such as a LFSR (linear feedback shift register), a reconfigurable core, a programmable logic block, a non-volatile RAM (e.g., magnetoresistive-RAM, ferroelectric-RAM), a matrix multiplier, and the like. Those of ordinary skill in the art will appreciate that other resources sets may also be included in the BN 212 without departing from the scope and spirit of the present invention.

[0040] The hardware/software system 202 may operate under the control of the secure protocol (i.e., protected protocol or encrypted protocol) 204 so that the hardware/software system 202 is actually set up and programmed by someone operating remotely by means of the secure protocol 204. By means of the secure protocol 204, a group of authorization information such as actual processing codes, keys (e.g., passwords), permissions, and metadata relating to the implementation of a DRM heuristic, and the like may be presented to the BN 214.

[0041] The trusted authority 206 may generate the secure protocol 204 which is preferably valid with respect to operations known to be supported by the BN 212. The trusted authority 206 may, for example, be a back-end server (which is assumed to be secure), a cell phone operator with a trusted command (and control center), an encrypted medium (which is assumed to be unique and uniquely in the possession of an authorized user of this particular instantiation of the architecture), or the like. The trusted authority 206 delivers the group of authorization information through the secure protocol 204 into

the BN 212. The trusted authority 206 may be in a vault. The trusted authority 206 may be operated according to some encryption or security measures.

[0042] One fundamental task of the BN 212 is to accept a key delivered through the secure protocol 204. The key may be presented in an encrypted form. Those of ordinary skill in the art will understand that various encryption, decryption and data-protection mechanisms may be utilized during the process of presenting and delivering the key. For example, digital watermarking, fast elliptical algorithms, Triple DES (also 3DES), and other contemporary algorithms may be utilized. In a preferred embodiment, the Rijndael algorithm is utilized.

[0043] The group of authorization information may be conveyed securely through the protocol 204 into the BN 212, which then operates and returns a result. The result may be used to activate an operation (e.g., playing a DVD medium) being authorized by means of an interaction between the secure protocol 204 and the BN 212. A critical aspect of this architecture 200 is the interaction that is set up between the trusted authority 206 and the BN 214 itself, and the activity that is set in motion by conveying the key and the relevant information through the secure protocol 204 into the BN 212.

[0044] According to the present invention, the BN 212 is unavailable to inspection by an attacker (e.g., a hacker) when the BN 212 is in operation. That is, although an attacker may grind the BN 212 down, photolithograph (or photomicrograph) the circuitry of the BN 212 at each level, and view the BN 212 in a static plan, the attacker is not able to inspect the BN 212 when the BN 212 is in operation.

[0045] Thus, even if an attacker, in principle, is able to inspect the secure protocol 204, inspect the software 210, inspect the process of the key and relevant information being presented by the software 210 to the microchip 208, and even potentially inspect the outer region 214 (i.e., all of the signals, all of the gates, all of the circuitry including the signal

lines between the BN 212 and the outer region 214, and the like, in the outer region 214), when the key and relevant information are presented to the BN 212, the attacker no longer has access. Therefore, all of the operations carried out by resource sets interior to the BN 212 are inaccessible to an attacker.

[0046] Since the key is deciphered inside the BN 212, and since the BN 212 is not accessible for inspection by an attacker when the BN 212 is in operation, the architecture 200 may thus defeat the attacker's attempt to get access to protected content.

(2) Grid Dribble Attack

[0047] FIG. 3 shows a derivative approach (grid dribble attack) to violating copyright on a digital medium. This form of attack is preferred by many hackers. A DVD 302 may contain an encrypted copy of content (e.g., movie, or the like). The DVD 302 is submitted to the Internet to a grid of computers 304. These computers 304 may be authorized users and have keys to decipher the encrypted content stored on the DVD 302. When these computers 304 apply decryption techniques to the encrypted movie on the DVD 302, correlated deciphered bits 306 of the movie may dribble out, bit by bit. It may take some time (e.g., six months) for the several hundreds of billions of bits that make up the target content to dribble out. However, once this happens, a perfect digital copy of the copyrighted content may then be presented on the Internet for unauthorized coping. Because there is no DRM system to ensure against this grid dribble attack which takes part in encryption mechanism bit by bit and dribbles out the results, content creators are extremely reluctant to make available digital content for general distribution.

[0048] FIG. 4 is a flowchart illustrating an exemplary process 400 for protecting against a grid dribble attack in accordance with the present invention. The process 400 may be implemented in the architecture 200 shown in FIG. 2.

[0049] The process 400 starts with a step 402 in which a BN is set in a quasi-stable mode (knife-edge stability). Among the resources architecture may make available include timer banks (essential for delivering quality service, e.g., high-quality digital video and audio). These timer banks are programmable. According to the present invention, the timer banks are set up in such a way that the timer banks may be presented with a bit string providing the time banks with certain pseudorandom temporal variability called a form jitter. Strictly speaking, the form jitter is not a jitter in an engineering term, but is a kind of pseudorandom variability that is knowable if one knows the bit string presented to the BN, which, in turn, is applied to the timer banks to set up the operation of the timer banks. Therefore, these timer banks are almost exactly right, but not exactly right.

[0050] According to the present invention, the bit string may be set up by one of the keys delivered by a secured protocol. Thus, in setting up a quasi-stable operation within the BN, one piece of information conveyed is preferably a key (for example, in a public key cryptosystem or a variant of a well-known public key cryptosystem). The key, instead of being applied to a difficult NP-hard problem (e.g., factoring very large prime numbers), is employed in conjunction with other keys to the creation of the quasi-stable BN mode of operation.

[0051] The quasi-stable mode of operation (step 402) means that an architecture is jittering ever so slightly and has an ability to compare its operation to the operation that would be dictated by one and only one such secret key presented to the timer banks. Such an ability provides a means for intrusion detection.

[0052] Next, in step 404 in the event of an attempt to invade the architecture, the clocking of some operations inside the BN may deviate (even if slightly) from the unpredictable but nevertheless well-known pattern of temporal behavior that is dictated by the key presented by the secure protocol, a mechanism may be triggered to stop the clock from running and cease the operation of the BN. In other words, upon the detection

of an intrusion, because the timing regime that has been set up is violated ever so slightly, the architecture basically stops working. This does not necessarily mean that the architecture as a whole ceases operation in the event of a detected intrusion because the architecture may start a re-buildup process (see step 406 below).

[0053] Next, in step 406, in the event of detected intrusion, the secure protocol, which is generated by the trusted authority, begins a process of re-establishing, through challenge and response, the buildup in a tiered hierarchical manner of a secure environment within the BN. If the attacker attempts to replicate this buildup, the attacker may only do it by having knowledge of the random characteristics of the secure protocol.

[0054] Thus, the architecture of the present invention is assailable only if both the BN and the trusted authority are compromised. Under extraordinary circumstances, such a thing may happen (as shown in FIG. 1, any architecture is theoretically breakable). In other words, hackers, burglars, thieves, or other unauthorized personnel may gain access to the trusted authority and one or more instances of the architecture under some extraordinary circumstances. When this happens, the clock is stopped and the attack effort is entirely reset to zero. That is, the validity of any element that might have eventuated from such an attack is completely nullified by the act of stopping the clock at this point. Therefore, intrusion, no matter how powerful the computational resources supplied to the intrusion, has the effect of resetting the effort involved to zero.

[0055] It is understood that there are thermodynamic principles that may permit an attacker, given sufficient determination, to override even this process 400. However, the reset-to-zero requirement and the proof against dribbling out bits in a concerted grid attack are more than ample to meet the needs of the great bulk of DRM requirements content creators have raised.

[0056] It is noted that although the architecture 200 shown in FIG. 2 and the process 400 shown in FIG. 4 are directed to the problem of DRM, they may also be applied to ATMs, other secured communications, TEMPEST requirements, or the like without departing from the scope and spirit of the present invention.

[0057] It is understood that the reliability aspect and the real-time behavior aspect relate to "knife-edge stability" described in the process 400 shown in FIG. 4. Those of ordinary skill in the art will appreciate that the interrelationship among security, reliability, and real-time behavior is intimately related in terms of how the resources are specified. In the architecture of the present invention, this interrelationship is exploited to create a very efficient architecture delivering the characterizable functions of the present invention.

[0058] It is to be noted that the above described embodiments according to the present invention may be conveniently implemented using conventional general purpose digital computers programmed according to the teachings of the present specification, as will be apparent to those skilled in the computer art. Appropriate software coding may readily be prepared by skilled programmers based on the teachings of the present disclosure, as will be apparent to those skilled in the software art.

[0059] It is to be understood that the present invention may be conveniently implemented in forms of software package. Such a software package may be a computer program product which employs a storage medium including stored computer code which is used to program a computer to perform the disclosed function and process of the present invention. The storage medium may include, but is not limited to, any type of conventional floppy disks, optical disks, CD-ROMS, magneto-optical disks, ROMs, RAMs, EPROMs, EEPROMs, magnetic or optical cards, or any other suitable media for storing electronic instructions.

[0060] It is understood that the specific order or hierarchy of steps in the processes disclosed is an example of exemplary approaches. Based upon design preferences, it is understood that the specific order or hierarchy of steps in the processes may be rearranged while remaining within the scope of the present invention. The accompanying method claims present elements of the various steps in a sample order, and are not meant to be limited to the specific order or hierarchy presented.

[0061] It is believed that the present invention and many of its attendant advantages will be understood by the foregoing description. It is also believed that it will be apparent that various changes may be made in the form, construction and arrangement of the components thereof without departing from the scope and spirit of the invention or without sacrificing all of its material advantages. The form herein before described being merely an explanatory embodiment thereof, it is the intention of the following claims to encompass and include such changes.